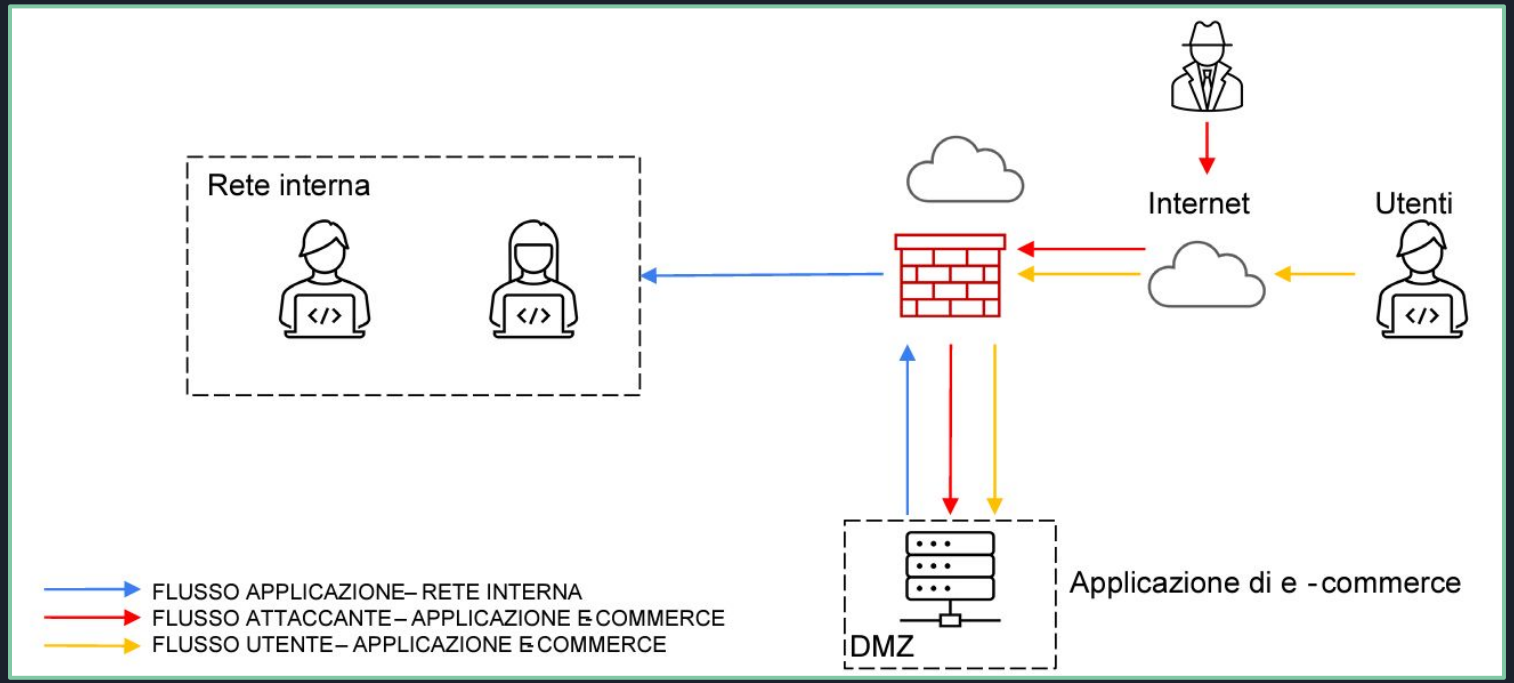
ANALISI DI SICUREZZA

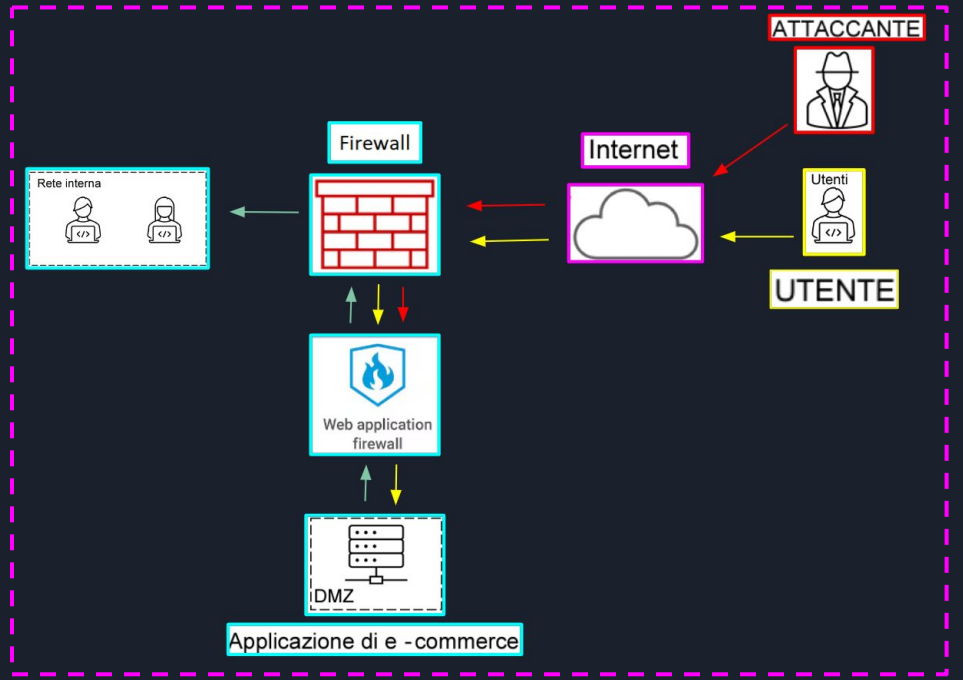
Kamenica Kristiano

ARCHITETTURA DELLA RETE



• Prevenzione attacchi SQLI E XSS

Al fine di mitigare i rischi derivanti da attacchi **SQLi** (*Injection di SQL*) ed **XSS** (*Cross-Site Scripting*), che potrebbero minacciare la sicurezza del nostro sistema, abbiamo implementato un **WAF** (*Firewall delle Applicazioni Web)* per proteggere il nostro server web. Stiamo attualmente valutando ulteriori misure preventive, tra cui la sanitizzazione degli input utente e il monitoraggio continuo del traffico di rete, al fine di rafforzare ulteriormente la sicurezza dei nostri sistemi. Inoltre, ti chiedo gentilmente di allegare il nuovo schema con il **WAF** implementato.



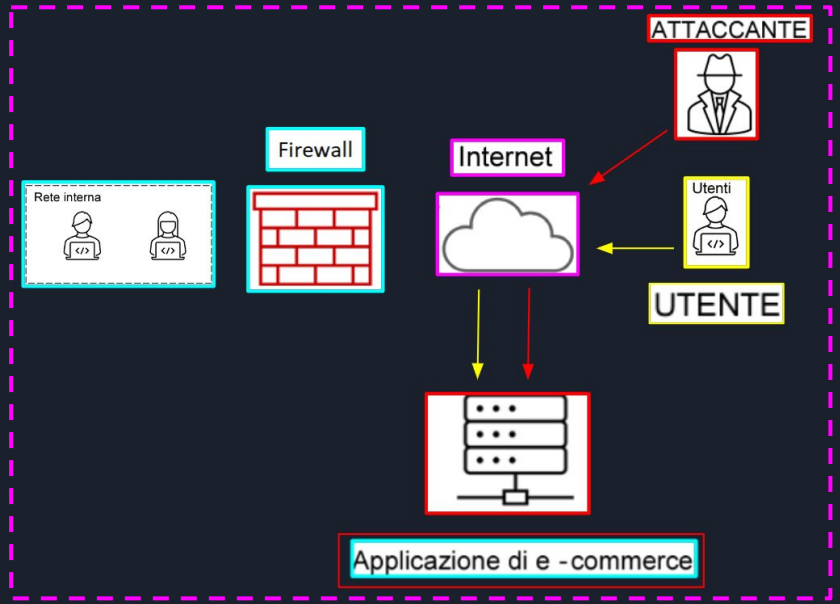
IMPATTO E PREVENZIONE DDOS

Nel caso di un ipotetico attacco **DDoS** (Distributed Denial of Service), si ipotizza che il servizio diventi irraggiungibile ai clienti per circa 10 minuti. Gli utenti spendono in media circa 1.500€ ogni minuto, sulla piattaforma. Con un semplice calcolo possiamo valutare una perdita di circa 15.000€ a fronte di un'interruzione di 10 minuti. Questa perdita potrebbe essere ridotta o evitata con un corretto **BCP** (Business Continuity Plan, piano di continuità operativa), che permetterebbe ad un servizio di continuare ad operare anche in situazioni critiche, tipo un attacco **DDoS**, danni accidentali o addirittura calamità naturali.

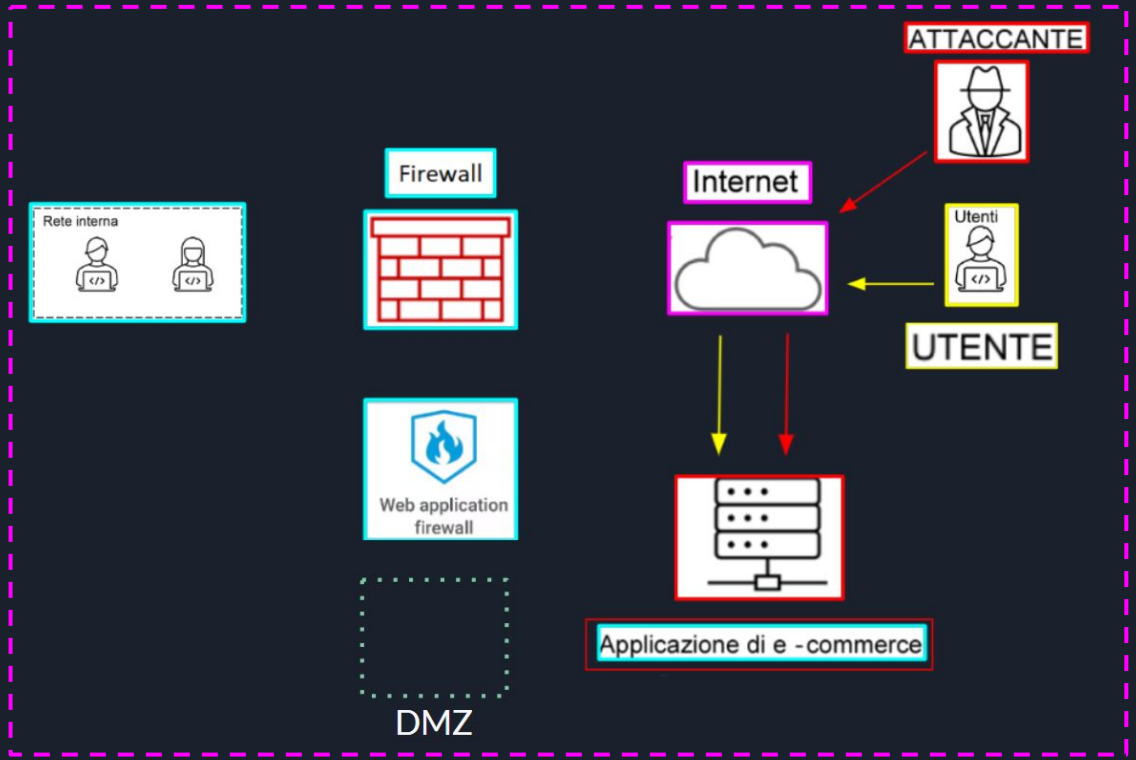
Un **BCP** valido si baserebbe sul identificare e pianificare i fattori di rischio, partendo da quelli più critici ed importanti (Risk Assessment), valutando l'impatto che questi avrebbero sull'azienda (BIA, Business Impact Analysis), formando il personale correttamente al fine di attuare il piano nel modo più efficiente e rapido possibile (per mantenere il servizio attivo al meglio delle possibilità), avendo a disposizione dei backup (possono essere strutture secondarie, sostituzioni di infrastrutture IT e via dicendo) ed infine migliorandolo e adattandolo costantemente per far fronte ai cambiamenti costanti, sia dentro, che fuori l'azienda.

• RESPONSE MALWARE

Per progettare l'integrazione della rete interna dell'azienda, abbiamo optato per l'isolamento come strategia principale. Questo approccio separa l'applicazione web dal resto dell'azienda, limitando il rischio di diffusione del malware nell'intera rete. È importante notare che, nonostante l'isolamento, un attaccante con accesso all'applicativo web dell'e-commerce potrebbe continuare ad avere accesso, rappresentando una possibile minaccia alla sicurezza.



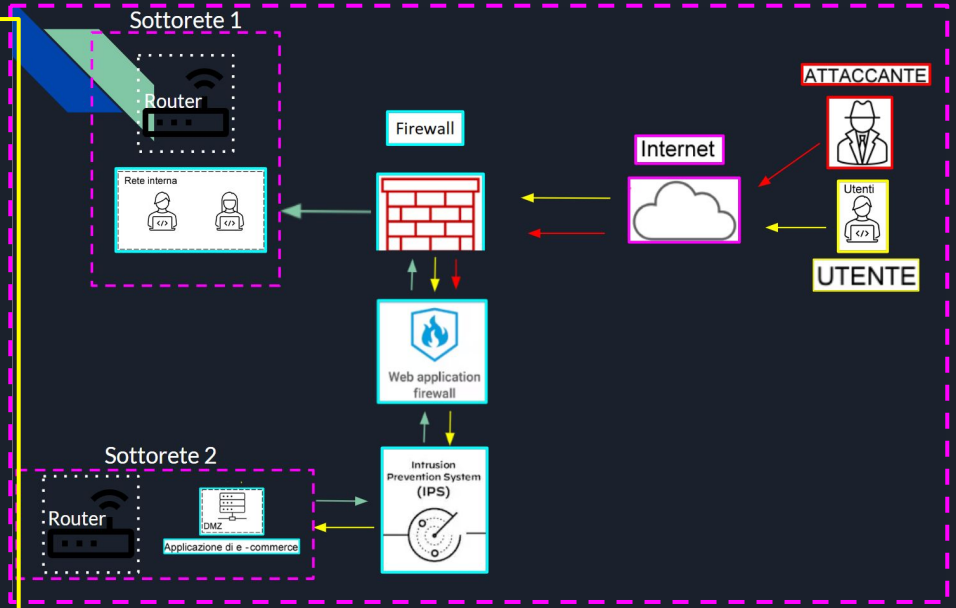
- **SOLUZIONE COMPLETA**



• MODIFICHE “AGGRESSIVE”

Per rafforzare ulteriormente la sicurezza dell'architettura dell'applicazione web e-commerce, abbiamo introdotto un sistema di Prevenzione delle Intrusioni (**IPS**) direttamente nel Web Server. Questo **IPS** monitora costantemente il traffico in ingresso e in uscita verso e dal server, identificando e bloccando eventuali tentativi di intrusioni o attacchi informatici. La presenza di un **IPS** a livello del Web Server aggiunge un ulteriore strato di protezione contro minacce come SQL Injection (**SQLi**), **Cross-Site Scripting** (**XSS**) e altri attacchi di livello applicativo.

Inoltre, per migliorare la gestione della rete e isolare meglio le diverse componenti del sistema, abbiamo suddiviso l'infrastruttura in sottoreti. Questa divisione ci consente di organizzare in modo più efficiente il traffico di rete e di limitare la superficie di attacco potenziale, aumentando così la resilienza del sistema alle minacce esterne. Ad esempio, abbiamo assegnato una subnet separata per il Web Server e un'altra subnet per le altre componenti dell'infrastruttura, consentendo un controllo più granulare sul flusso di dati e una migliore gestione delle politiche di sicurezza.



• BONUS 1

LINK

COS'E:

- "PERFORMANCE_BOOSTER_v3.6.exe" è un file che sembra promettere di migliorare le prestazioni del computer, ma in realtà è dannoso.

COSA FA:

- Modifica le impostazioni di sicurezza di PowerShell per eseguire comandi dannosi senza restrizioni.
- Legge informazioni sensibili dal registro di sistema, come la cronologia delle connessioni remote e le impostazioni di Internet.
- Modifica i file per nascondere la sua presenza.

PERICOLOSITÀ:

- Può danneggiare il sistema, rubare informazioni sensibili o consentire l'accesso non autorizzato al computer.

SOLUZIONE:

- Rimuovere immediatamente il file "PERFORMANCE_BOOSTER_v3.6.exe" dal computer.

• BONUS 2

LINK

COS'E:

- Un malware che si camuffa come programma di aggiornamento di browser microsoft(Edge)

COSA FA:

- Il software dannosa rilascia dei file che si eseguono automaticamente all'avvio del sistema.
- Agisce come un processo di Windows, quindi e in grado operazione in background senza il consenso dell'utente.
- Può modificare il sistema e accedere a impostazioni di rete e sicurezza.
- Comunica con diversi server online, cio puo indicare un tentativo di trasmettere dati sensibili o riceve istruzione da fonti remote.

PERICOLOSITÀ:

- Agisce in modo furtivo e può manipolare file e comunicare con server remoti.

SOLUZIONE:

- Scansione Antivirus per individuare il Malware e rimuoverlo.